



Office de la propriété
Intellectuelle
du Canada

Un organisme
d'Industrie Canada

Canadian
Intellectual Property
Office

An Agency of
Industry Canada

ICTICA 03/00049

29 JANUARY 2003 29.01.03

#2

REC'D 17 FEB 2003

PCT

*Bureau canadien
des brevets
Certification*

*Canadian Patent
Office
Certification*

La présente atteste que les documents
ci-joints, dont la liste figure ci-dessous,
sont des copies authentiques des docu-
ments déposés au Bureau des brevets.

This is to certify that the documents
attached hereto and identified below are
true copies of the documents on file in
the Patent Office.

Mémoire descriptif et dessin, de la demande de brevet no: 2,367,309, tel que déposé le
17 janvier 2002, par MICHEL CARON, ayant pour titre: "Carte à Puce Fournissant un
Numéro Transactionnel Unique et Différent pour Chaque Utilisation de Son Détenteur".

**PRIORITY
DOCUMENT**

SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

Tracy Paulhus
Agent certificateur/Certifying Officer

BEST AVAILABLE COPY

29 janvier 2003

Date

BEST AVAILABLE COPY

Canada

(CIPO 68)
04-09-02

OPIC  CIPO

ABRÉGÉ DE L'INVENTION

Un appareil fournissant un numéro de transaction unique et différent pour chaque utilisation de son détenteur. Cet appareil a une carte munie de touches et d'un écran. Il a aussi un circuit électronique intégré dans la carte. Enfin, celui-ci a un programme faisant fonctionner le circuit électronique de façon à recevoir un code entré à l'aide des touches de la carte par le détenteur et affichant le numéro de transaction unique à l'écran.

**CARTE À PUCE FOURNISSANT UN NUMÉRO TRANSACTIONNEL
UNIQUE ET DIFFÉRENT POUR CHAQUE UTILISATION DE SON
DÉTENTEUR.**

RÉSUMÉ DE L'INVENTION

5 La présente invention concerne un appareil fournissant un numéro de transaction unique et différent pour chaque utilisation de son détenteur, comprenant:

 une carte munie de touches et d'un écran;

 un circuit électronique intégré dans la carte; et

10 un programme faisant fonctionner le circuit électronique de façon à recevoir un code entré à l'aide des touches de la carte par le détenteur et affichant le numéro de transaction unique à l'écran.

BRÈVE DESCRIPTION DE LA FIGURE

15 La figure 1 est une vue de face d'une carte à puce fournissant un numéro transactionnel selon une réalisation préférentielle de la présente invention.

DESCRIPTION DÉTAILLÉE DE L'INVENTION

20 La SECUR-CARD (1) (nom préliminaire de l'invention) est un appareil ayant pour but l'élimination des fraudes par carte de crédit et carte de débit. Concrètement la SECUR-CARD (1) est une carte à puce, interactive, munie d'un écran (2) d'affichage semblable à celle des calculatrices. Ces six touches permettront à son détenteur une utilisation tout à fait sécuritaire. Nous verrons plus loin une description de chacune de ses six touches.

La SECUR-CARD (1) fonctionnera de concert avec les cartes de crédit et

de débit de son détenteur. Aucune transaction ne sera possible avec lesdites cartes de crédit ou de débit sans donner le numéro (10) transactionnel fourni par la SECUR-CARD (1). La SECUR-CARD (1) donnera un numéro différent pour chacune des transactions faites par son détenteur.

LA SECUR-CARD (1) EST-ELLE UNE CARTE DE CRÉDIT?

Non! Même si elle aura la taille d'une carte de crédit, elle sera distincte de toute carte de crédit ou de débit. La SECUR-CARD (1) aura l'apparence d'une mini calculatrice. Les consommateurs la verront comme LA garantie de sécurité pour toutes transactions commerciales ou bancaires faites avec leurs cartes de crédit ou de débit.

Pour pouvoir se servir de la SECUR-CARD (1) il faudra entrer un NIP (numéro d'identification personnel) à l'aide d'un clavier (4-5) sécurisé (voir détails plus loin). La SECUR-CARD (1) fonctionne à l'aide d'une puce électronique qui agit comme chiffrier et gestionnaire de dossiers. Son rôle est de fournir un numéro (10) transactionnel différent pour chacune des transactions faites par son détenteur. Le calcul pour fournir ce numéro(10) unique est fait à partir du numéro officiel d'une carte de crédit ou de débit et d'un code secret.

Les compagnies émettrices de ces cartes autoriseraient une transaction qu'après avoir validé le numéro (10) de transaction fourni par la SECUR-CARD (1). Pour ce faire, elles effectueraient le même calcul que celui effectué par la SECUR-CARD (1) pour le client. C'est le consommateur qui transmettrait ce numéro(10) transactionnel manuellement avec les claviers numériques qui sont déjà chez les commerçants.

Il est important de comprendre que la SECUR-CARD (1) n'aura aucun lien physique avec les compagnies émettrices de cartes. Si ce n'est que son

détenteur entrera dans la banque de données de sa SECUR-CARD (1) le numéro officiel de sa carte de crédit et/ou de débit ainsi qu'un code secret. Ces informations seront aussi connues des systèmes centraux des compagnies émettrices, mais en aucun moment il ne sera établi un lien de communication entre la SECUR-CARD (1) et lesdites compagnies.

Cette carte à puce sera donc de type "fermée", c'est-à-dire qu'elle ne pourra être lu par aucun lecteur de carte à puce: Ceci pour éviter qu'un fraudeur puisse lire les informations (numéro de carte et code secret) comprises à l'intérieur de la puce électronique. La puce n'est là que pour servir de chiffrier pour exécuter l'algorithme fournissant le numéro (10) transactionnel. La SECUR-CARD (1) ne fera qu'afficher ce numéro (10) sur son écran (2).

Pour les transactions sur internet, le consommateur transmettra le numéro d'identification de sa carte de crédit (qui est différent du numéro officiel de la carte de crédit) et le numéro (10) transactionnel. Le consommateur pourra le faire sans crainte car ce numéro (10) transactionnel n'est valide que pour une seule transaction. Le même fonctionnement prévaudrait pour les transactions téléphoniques.

Le numéro d'identification de la carte de crédit ne pourra, seul, servir à effectuer une transaction: il devra toujours être jumelé au numéro (10) transactionnel fourni par la SECUR-CARD.

Une seule SECUR-CARD(1) pourra fournir les numéros (10) transactionnels pour différentes cartes de crédit ou de débit détenues par son propriétaire. Pour ce faire, la puce électronique pourra gérer plusieurs dossiers différents selon les besoins de son détenteur.

Puisque les numéros officiels des cartes de crédit et de débit sont tous différents les uns des autres, ainsi que les numéros de code secret qui les

4

accompagneront, la SECUR-CARD (1) émettra un numéro (10) différent pour chacune des transactions effectuées par chacune des cartes (crédit ou débit) de son détenteur.

CONSÉQUENCE

- 5 Une sécurité absolue: un fraudeur qui obtiendrait le numéro (10) de transaction(par quelques moyens que ce soit) ne pourrait l'utiliser pour effectuer un autre achat. Après une seule transaction ce numéro (10) devient automatiquement invalide. Même en possession de la carte de notre membre et de sa SECUR-CARD(1), le fraudeur ne pourrait transiger,
- 10 car il n'aurait pas le NIP permettant la mise en fonction de la SECUR-CARD(1).

EFFICACITÉ

- 15 Cette nouvelle approche fonctionne aussi bien pour des transactions conventionnelles ou sur internet que celles effectuées par téléphone. Elle peut même être utilisée, comme démontré plus loin, pour les cartes de débits.

- 20 Pour activer la SECUR-CARD(1) lors de sa réception, le titulaire devra effectuer à l'aide du clavier(4-5) sécurisé les trois opérations suivantes:

- 1- Entrer le numéro de sa carte de crédit ou de débit qui sera indiqué dans la lettre accompagnant sa nouvelle carte.
- 25 2- Entrer le code secret de 6 chiffres qu'il aura préalablement détaché du formulaire d'adhésion lors de sa demande.
- 3- Se choisir et ensuite entrer un NIP de 4 chiffres.

5

Les deux premières opérations ne seront effectuées qu'une seule fois: à l'activation de la SECUR-CARD (1). Par la suite, lorsque le consommateur voudra effectuer une transaction, il n'aura qu'à mettre sa SECUR-CARD (1) en marche, indiquer pour quel dossier il veut effectuer une transaction (VISA, MASTERCARD ou carte de débit...) celle-ci lui demandera ensuite d'inscrire son NIP. Une fois fait, la SECUR-CARD (1) effectuera automatiquement un calcul pour obtenir le seul numéro (10) valide pour cette transaction.

Voici un exemple simplifié.

Michel Caron a demandé une nouvelle carte de crédit VISA et pour la première fois il s'est inscrit au programme SECUR-CARD (1). Lors de la réception de sa nouvelle carte de crédit VISA, dans l'enveloppe accompagnant sa carte, il trouve une lettre explicative ET la SECUR-CARD (1). Dans la lettre il est inscrit que le numéro de sa nouvelle carte VISA est le 324. Bien entendu ce numéro n'est inscrit ni sur la carte de crédit, ni sur la bande magnétique de celle-ci. Le numéro gravé sur la carte VISA et transcrit sur sa bande magnétique n'est qu'un numéro d'identification. En aucun cas ce numéro pourra servir à autoriser une quelconque transaction.

M.Caron suit les instructions: met sa SECUR-CARD(1) en marche, apparaît à l'écran(2) «dossier 1 2 3 4 5» avec un curseur(9) sous le numéro 1. Puisque M.Caron en est à son premier dossier pour sa SECUR-CARD(1), il appuie sur la touche(7) «ENTER», pour pouvoir entrer les informations dans le dossier numéro «1». S'il avait déjà des dossiers actifs dans sa SECUR-CARD(1), M.Caron aurait choisi, à l'aide du clavier(4-5) sécurisé, le prochain numéro de dossier disponible.

Ensuite à l'aide du clavier(4-5) sécurisé il entre son numéro de carte 324, son code secret 523 527 (qu'il a détaché de la formule d'adhésion lorsqu'il a rempli ladite formule) et se choisit un NIP. Il est maintenant prêt à faire une première transaction.

5

Il va à la station-service pour effectuer le plein d'essence de sa voiture. Après son achat, il présente sa carte de crédit pour payer. Le commis passe sa carte dans le lecteur et inscrit le montant de la transaction. L'ordinateur central de VISA reconnaît la carte de Michel Caron par son numéro d'identification. Il demande alors à celui-ci de lui fournir le seul numéro(10) de transaction possible pour cet achat.

10

M.Caron sort sa SECUR-CARD(1), la met en marche, il apparaît à l'écran(2) «dossier 1 2 3 4 5». À l'aide du clavier(4-5) il choisi le dossier «1» et appuie sur «ENTER». La SECUR-CARD(1) lui demande son NIP, ce qu'il s'empresse de faire, apparaît alors sur l'écran(2) de la SECUR-CARD(1) le numéro(10) 473. À l'aide du clavier numérique du commerçant, il inscrit le # 473. Si le clavier du commerçant n'est pas accessible aux consommateurs M.Caron dirait ce numéro(10) tout simplement à vive voix au commerçant. Il pourra le faire sans crainte car ce numéro(10) n'est valide que pour cette seule transaction. La compagnie VISA acceptera la transaction, car elle sait que le seul numéro(10) possible pour autoriser cette transaction est bien le numéro 473.

15

20

25

Mais d'où vient ce numéro(10) 473?

Dans cet exemple simplifié, le numéro de carte VISA de Michel Caron est le 324, son code secret est le 523 527. Il est établi dans la puce électronique de la SECUR-CARD (1) que pour tous les détenteurs du code 523 527, le numéro (10) autorisant la première transaction est l'addition du nombre 149 avec le numéro de carte VISA. Sachant que le numéro de la carte de crédit

30

de M.Caron est le 324, alors nous avons l'équation suivante: $149+324$ qui donne comme résultat 473.

5 Puisque l'ordinateur de la compagnie VISA connaît aussi bien le numéro de carte que le code secret de M.Caron, et l'algorithme utilisé, il aura effectué le même calcul pour arriver au même résultat.

10 Pour la deuxième transaction, de M.Caron, le numéro à additionner au numéro de carte est le 381. Donc, $381+324=685$. Si quelqu'un voulait effectuer une transaction avec la carte de M.Caron, il ne le pourrait pas car il ignorerait que le seul numéro(10) autorisant cette transaction est le 685.

15 Un chiffre différent étant additionné au numéro de carte pour chacune des transactions, cela rendra la fraude presque impossible.

20 Il est important de noter que ni le numéro de carte de crédit ni le chiffre devant s'additionner à celui-ci n'apparaîtront à l'écran(2) de la SECUR-CARD: Seul le résultat apparaît à l'écran(2). Pour la première transaction il n'y apparaîtra que le numéro(10) 473 et pour la deuxième, seul le numéro(10) 685 apparaîtra sur l'écran(2) de la SECUR-CARD(1). Il sera impossible de prévoir le numéro(10) suivant.

25 Il est bien entendu que le véritable algorithme employé par la SECUR-CARD(1) sera plus complexe que celui démontré dans cet exemple simplifié qui ne sert qu'à présenter le procédé de fonctionnement.

30 Pour une transaction effectuée à l'aide d'une carte de débit, le procédé est identique. Le numéro(10) transactionnel fourni par la SECUR-CARD(1) remplace dans le système central de la compagnie émettrice le numéro de NIP qui est demandé à l'heure actuelle. Mais contrairement au numéro de NIP actuel, le numéro(10) fourni par la SECUR-CARD(1) change après chaque transaction. Les clients ne seront plus inquiets de savoir qu'une

autre personne peut voir le numéro(10) qu'ils poinçonnent sur le clavier du commerçant ou sur celui du guichet automatique.

Qu'est-ce que le clavier(4-5) sécurisé?

5 Contrairement à ce qui se fait à l'heure actuelle, le clavier(4-5) sécurisé de la SECUR-CARD(1) pour entrer les données essentielles (numéro de carte de crédit, code secret, NIP etc) ne serait pas alphanumérique. Ce clavier(4-5) sécurisé serait composé principalement de deux touches identifiées par deux flèches(4-5). Ces touches(4-5) serviraient à déplacer un curseur(9)
10 apparaissant à l'écran(2) de la SECUR-CARD(1). Une touche pour aller vers la gauche(4) et l'autre pour aller vers la droite(5).

 Bien sûr, il y aurait d'autres touches(6-7-8-11) sur la SECUR-CARD(1). Ces autres touches(6-7-8-11) sont respectivement: «ON/OFF»(6) pour la mise
15 en marche de la SECUR-CARD(1), «ENTER»(7) pour valider une entrée, «CLEAR»(8) pour annuler la dernière entrée et finalement «M»(11) pour choisir entre une transaction manuelle ou automatisée. Mais ces touches(6-7-8-11) n'ont rien de révolutionnaire. Regardons comment les touches(4-5) innovatrices de la SECUR-CARD rendent les transactions beaucoup plus
20 sécuritaires. Voici un exemple simple de son fonctionnement:

 M.Caron a déjà activé sa SECUR-CARD(1). Il est chez un commerçant et veut effectuer une transaction. Il met en marche sa SECUR-CARD(1) en appuyant sur la touche «ON/OFF»(6), puisque M.Caron n'a qu'un dossier
25 dans sa SECUR-CARD(1), il pèse immédiatement sur «ENTER»(7) pour indiquer qu'il veut un numéro dans le dossier numéro «1». Alors apparaît à l'écran(2) de sa SECUR-CARD(1) «indiqué votre NIP». M.Caron appuie sur la touche «ENTER»(7), alors apparaît à l'écran(2) un curseur(9). Ce curseur(9) est arrêté au-dessus d'un des chiffres(3) imprimés juste en
30 dessous de l'écran(2): «1 2 3 4 5 6 7 8 9 0» . Pour une sécurité maximale, le curseur(9) n'apparaît jamais au-dessus du même chiffre(3). Il peut

apparaître au-dessus du 1 et la fois suivante apparaître, de façon aléatoire, au-dessus du 5 ou du 8 etc.

5 Pour notre exemple le NIP de M.Caron est 6384. Le curseur(9) est apparu au-dessus du chiffre(3) 2. Puisque le premier chiffre composant le numéro du NIP est le 6, M.Caron appuie quatre fois sur la flèche(5) de droite pour amener le curseur(9) au-dessus du chiffre(3) 6. Il appuie sur la touche «ENTER»(7) pour valider ce premier chiffre.

10 Le curseur(9) disparaît momentanément de l'écran(2) et réapparaît au-dessus d'un autre chiffre(3), encore une fois ce chiffre(3) est choisi de façon aléatoire. Apparaît au même moment sur l'écran(2) un symbole comme celui-ci: «*» pour indiquer que le premier chiffre composant le NIP a été sélectionné. Bien sûr ce symbole «*» apparaîtra deux fois pour indiquer que les deux premiers chiffres du NIP ont été sélectionnés, ainsi de suite. Poursuivons notre exemple, le curseur(9) réapparaît au-dessus du
15 chiffre(3) 9, M.Caron appuie à six reprises sur la flèche(4) de gauche pour amener le curseur(9) au-dessus du chiffre(3) 3. Puisque le deuxième chiffre composant son NIP est bien le 3, il appuie sur la touche «ENTER»(7) pour valider ce chiffre. Le même processus recommence pour le choix du troisième et du quatrième numéro de son NIP. S'il avait fait une erreur en appuyant sur le bouton «ENTER»(7) trop rapidement, il n'aurait qu'à peser
20 sur le bouton «CLEAR»(8) pour annuler la dernière entrée, faire la correction et poursuivre.

25 Aujourd'hui, il est facile pour un fraudeur bien entraîné de connaître le NIP d'un client juste en regardant celui-ci le composer sur le clavier du commerçant.

30 Même ce nouveau clavier(4-5) sécurisé, ne serait pas à l'abri des regards indiscrets si le curseur se positionnerait toujours sur le 1, il serait possible pour un fraudeur attentif de compter le nombre de fois que le client a

appuyé sur la flèche(5) de droite, par exemple 5 fois, pour déplacer le curseur(9) au-dessus du premier chiffre de son NIP. Le fraudeur saurait alors que le premier chiffre du NIP est le 6. Ainsi de suite pour les autres numéros.

5

Avec cette nouvelle façon de faire, un fraudeur, même à l'affût, placé près de M.Caron ne pourrait le voir appuyer sur les chiffres composant son NIP. Tout ce qu'il pourrait voir, c'est M.Caron appuyant sur des flèches(4-5) pour déplacer un curseur(9), qui lui, ne se positionnerait jamais au-dessus du même chiffre pour débiter une nouvelle sélection, d'où une sécurité de transaction accrue.

10

Nous venons de décrire l'utilisation régulière de la SECUR-CARD(1). C'est-à-dire chez les commerçants ayant un lien, en temps réel, avec les compagnies de cartes de crédit et de débit.

15

Par contre, en tant que consommateur, nous avons à faire, à l'occasion, avec des petits commerçants qui fonctionnent encore de façon manuelle. Concrètement, ils prennent l'empreinte de la carte de crédit de leurs clients et les envoient chez les compagnies émettrices à intervalle plus ou moins régulier.

20

Bien entendu avec la SECUR-CARD(1), il est important que la compagnie émettrice connaisse en temps réel les transactions effectuées par le détenteur de la SECUR-CARD(1). Comme démontré plus haut, le numéro(10) change pour chacune des transactions faites par le détenteur. Si M.Caron effectue 3 transactions chez autant de commerçants qui sont reliés au système central de VISA, celui-ci pourra valider facilement chacune de ces transactions car il saura, en tout temps, à quelle séquence M.CARON est rendu.

25

30

Par contre pour que M.Caron puisse faire une transaction chez un

commerçant qui n'est pas relié au système de VISA, la SECUR-CARD(1), doit pouvoir lui fournir aussi un numéro de transaction différent. Pour ce faire, M.Caron avant d'inscrire son NIP à l'aide du clavier(4-5) sécurisé, pèsera sur la touche «M»(11) pour obtenir un numéro(10) spécifique aux transactions faites de façon manuelles sans vérification.

5

En effet deux séries différentes de numéro(10)d'autorisation seront fourni par la SECUR-CARD(1). Une pour les transactions automatisées et une pour les transactions manuelles. De cette façon, VISA, dans notre exemple, pourra valider chacune des transactions automatisées de son client, et lorsque les relevés manuels des transactions lui parviendront, elle pourra les valider, elles aussi, avec leurs numéros(10) de transactions propres. Bien entendu si M.Caron effectue plus d'une transaction manuelle, chacune d'entre elle se sera vu octroyer un numéro(10) de transaction différent.

10

Il va de soi que de nombreuses modifications pourraient être apportés aux modes de réalisation qui viennent d'être décrits sans sortir du cadre de la présente invention telle que définie dans la revendication annexée.

15

REVENDEICATION

1. Un appareil fournissant un numéro de transaction unique et différent pour chaque utilisation de son détenteur, comprenant:

une carte munie de touches et d'un écran;

5

un circuit électronique intégré dans la carte; et

un programme faisant fonctionner le circuit électronique de façon à recevoir un code entré à l'aide des touches de la carte par le détenteur et affichant le numéro de transaction unique à l'écran.

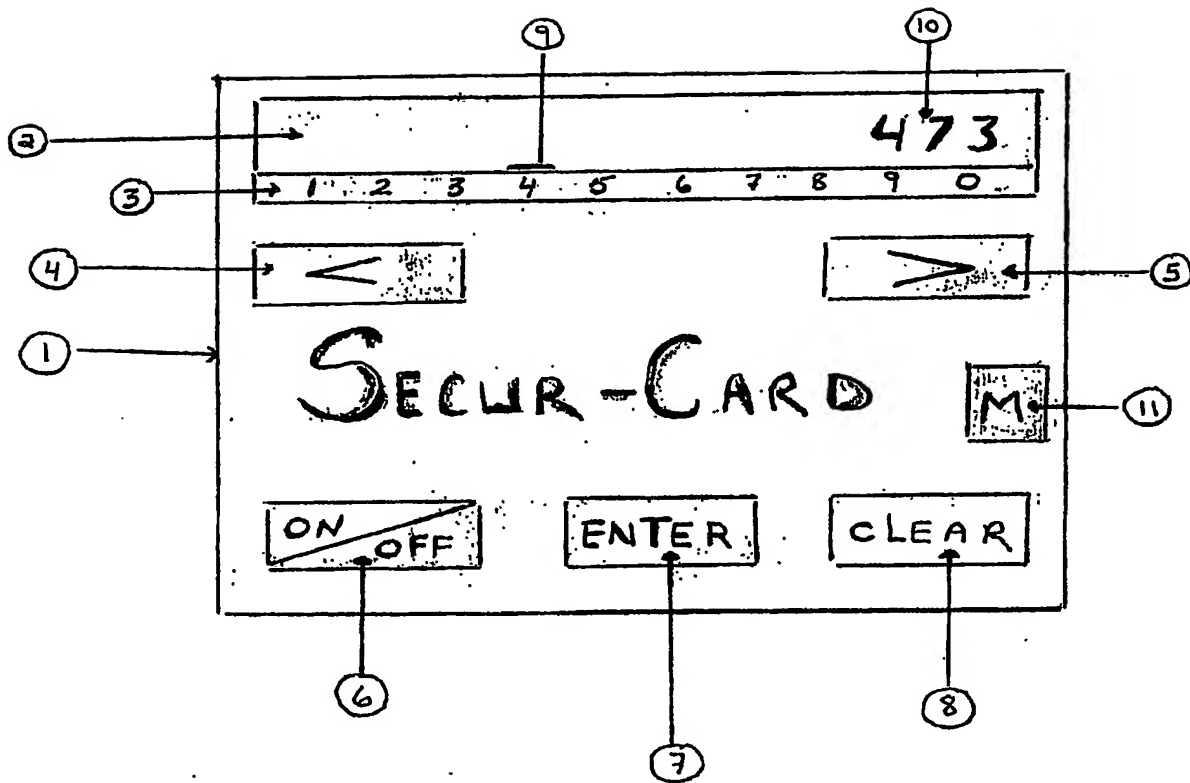


FIGURE 1

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.